UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In re Flagstar December 2021 Data Security Incident Litigation

Case No. 22-cv-11385

_____/

Hon. Brandy R. McMillion

OPINION AND ORDER DENYING IN PART AND GRANTING IN PART DEFENDANT'S MOTION TO DISMISS (ECF NO. 58)

Plaintiffs John Scott Smith, Christopher P. Kennedy, Erin Tallman, Mark Wiedder, Michael McCarthy, Rafael Hernandez, William Worton, Hassan Nasrallah, Nathan Silva, Laurie Ewing Scanlon, Everett Turner, and Allie McLaughlin ("Plaintiffs") filed this consolidated action, on behalf of themselves and all other similarly situated persons, against Defendant Flagstar Bancorp, Inc. ("Flagstar") for violations of their privacy rights stemming from their personally-identifiable information ("PII") being compromised in a data breach Flagstar experienced in December 2021 (hereinafter, "the Data Breach" or "the Flagstar Breach"). ECF No. 52, PageID.562.

The heart of Plaintiffs' allegations is that the Data Breach was a result of Flagstar's failure to adequately protect Plaintiffs' PII. *See* ECF No. 52, PageID.545. Because of Flagstar's failure, Plaintiffs' PII was exfiltrated, held for ransom by the

cyber attackers, and ultimately "made available to other criminals on the dark web." *Id.* at PageID.547. Since having their PII compromised in the Data Breach, Plaintiffs have suffered numerous injuries including, *inter alia*, fraud and identity theft, loss of value of their PII, ongoing threat of certain, imminent harm, and the cost of identity defense and credit monitoring services to mitigate these future harms. *Id.* at PageID.586.

Flagstar filed a Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint. *See* ECF No. 58. Flagstar moves for dismissal on the grounds that Plaintiffs lack Article III standing and fail to state a claim. *Id.* at PageID.671. Plaintiffs responded and the motion is fully briefed. *See* ECF Nos. 72, 75. The Court held a motion hearing on September 23, 2024. *See* ECF No. 86. For the reasons below, the Court **DENIES IN PART**, and **GRANTS IN PART**, Defendant Flagstar's Motion to Dismiss. ECF No. 58.

I.

Flagstar is a stock savings bank with its corporate headquarters in Michigan. ECF No. 52, PageID.547. In order to operate its business, Flagstar "collects, maintains, and profits from the PII" of all its customers. *Id.* at 557. PII is "information that is used to confirm an individual's identity and can include an individual's name, Social Security number, driver's license number, phone number, financial information, and other identifying information unique to an individual."

Id. Flagstar stores its data on centralized servers it maintains itself. *Id*. at 558. Aware of the "potentially serious threat" of fraud that comes with maintaining such highly sensitive information, Flagstar assures its customers that it is "committed to [their] financial security" and that they "closely monitor[s] all types of white-collar crime, including identity theft and . . . fraud." *Id*. at PageID.560-561 (citing Flagstar.com). Flagstar also informs its customers of its "firewalls and prevention systems" that are meant to stop unauthorized access to the Flagstar networks. *Id.* at PageID.561.

The December 2021 Cyber Attack

On December 3rd and 4th, 2021, cyber attackers hacked Flagstar's network and accessed the PII of 1.5 million customers. *Id*. at PageID.562. Flagstar publicly announced the Data Breach on June 17, 2022 after finishing "an extensive forensic investigation and manual document review on June 2, 2022." ECF No. 52, PageID.562-563. It did not notify any customers who had PII compromised in the Data Breach before then. *Id.* at PageID.563. Flagstar also notified compromised customers through individual breach notification letters. *Id.* at 564. The letters stated that Flagstar had "no evidence that any of your information has been misused." *Id.* at PageID.565. Flagstar offered its customers "two years of credit monitoring and identity protection services" in response to the breach. *Id.* at PageID.564. It also cautioned its customers to place "a fraud alert and/or security

freeze on [their] credit files to help protect your personal information." *Id.* at PageID.566.

Plaintiffs allege numerous injuries as a result of this PII being compromised;[1] the specific allegations of the named Plaintiffs can be found in the Consolidated Class Action Complaint. ECF No. 52, PageID.547-556. Importantly, some Plaintiffs were notified that their PII was located on the dark web, and all Plaintiffs have had to continue purchasing credit monitoring services as a result of this breach. *Id.*

The Ransom Negotiations[2]

Cyber attackers began infiltrating Flagstar's network as early as November 22, 2021. ECF No. 72, PageID.1491. They exfiltrated "massive amounts of PII" from Flagstar's network" over the two-day period in December. *Id.* The cyber

[1] "Plaintiffs and Class Members were injured as follows: i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of access to Plaintiffs' and Class Members' PII permitted by Flagstar; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach; (vi) Flagstar's retention of profits attributable to Plaintiffs' and Class Members' PII that Flagstar failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non- economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to Flagstar for services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and (x) nominal damages." ECF No. 52, PageID.586.

[2] Plaintiffs were not aware of the fact that this was a ransomeware attack nor that Flagstar had engaged in ransom negotiations, thus, no ransom allegations appear in the Complaint. *See generally* ECF No. 52. The Court therefore uses information provided by Defendant Flagstar in its Motion to Dismiss and accepted by Plaintiffs in their responsive brief. *See* ECF Nos. 58, 72. Where the information is contested by the parties, the Court will so note.

attackers demanded ransom for return of the stolen data. *Id.* After engaging in ransom negotiations through a hired external cybersecurity professional (Tetra Defense, Inc.), Flagstar agreed to pay the ransom. ECF No. 58, PageID.690. In exchange for the ransom payment, Flagstar requested, among other things, "the complete deletion of all data acquired from Flagstar's network." *Id.* Flagstar completed payment and deletion of all the compromised data on December 31, 2021. *Id.* Flagstar also sought assurances from the cyber attackers that there were no additional copies of the data that had been taken and that it had deleted as part of the ransom payment; the cyber attackers did not explicitly confirm there were no copies. ECF No. 72, PageID.1495-1496.

Flagstar hired two cybersecurity vendors to monitor the dark web in October 2022 and found "no evidence that the [cyber attackers] released any Flagstar data" from this data breach. *Id.* at PageID.1498-1499. However, some of named Plaintiffs' data was located on the dark web. According to one of Flagstar's cybersecurity experts, this was "data from the Accellion Incident"—a breach Flagstar customers had been compromised in when a ransomware gang targeted the servers of Accellion (a vendor Flagstar used). ECF No. 52, PageID.568; ECF No. 58, PageID.693.

The Current Action

Named plaintiffs began filing individual suits against Flagstar in June 2022, soon after Flagstar publicly announced the breach. *See* ECF No. 1. Plaintiffs' cases were consolidated and they filed their Consolidated Class Action Complaint on June 23, 2023. ECF No. 52. Plaintiffs bring eighteen claims against Flagstar: Negligence (Count I); Negligence Per Se (Count II); Unjust Enrichment (Count III); Breach of Confidence (Count IV); Invasion of Privacy – Intrusion Upon Seclusion (Count V); Breach of Express Contract (Count VI); Breach of Implied Contract (Count VII); Declaratory Judgment (Count VIII); California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.150, *et seq*. (Count IX); California Customer Records Act ("CCRA"), Cal. Civ. Code §§ 1798.80, *et seq*. (Count X); California Unfair Competition Act ("ULC"), Cal. Bus. & Prof. Code §§ 17200, *et seq*. (Count XI); California Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, *et seq*. (Count XII); Colorado Security Breach Notification Act, Colo. Rev. Stat. §§ 6-1-716, *et seq*. (Count XIII); Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101, *et seq*. (Count XIV); Indiana Deceptive Consumer Sales Act ("IDCSA"), Ind. Code § 24-5-0.5 (Count XV); Michigan Consumer Protection Act ("MCPA"), Mich. Comp. Laws Ann. § 445.901 *et seq*. (Count XVI); Washington Data Breach Notice Act ("WDBNA"), Wash. Rev. Code Ann. § 19.255.010 (West) (Count XVII); Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code §§

19.86.020, *et seq*. (Count XVIII). *See id.* Flagstar filed its Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint on July 24, 2023, arguing that Plaintiffs lack Article III standing and fail to state a claim as to any of their eighteen counts. *See* ECF No. 58. The motion was fully briefed, and the Court heard oral argument on Monday, September 30, 2024. ECF No. 86.

For the reasons set forth, the Court **GRANTS** Flagstar's Motion to Dismiss as to Counts I, II, III, IV, V, VI, VII, VIII, X, XI, XII, XIII, XIV, XV, XVI, XVII, and XVIII; and **DENIES** Flagstar's Motion to Dismiss as to Count IX.

II.

Flagstar moved to dismiss under Federal Rule of Civil Procedure 12(b)(1) or alternatively under Rule 12(b)(6). A motion under 12(b)(1) challenges a court's subject-matter jurisdiction over claims presented. Fed. R. Civ. P. 12(b)(1). Such a motion attacks jurisdiction either facially or factually. *United States v. Ritchie*, 15 F.3d 592, 598 (6th Cir. 1994). Defendants' challenge the Court's subject-matter jurisdiction under a facial attack and a facial attack. A facial challenge requires the Court to accept as true the allegations in the pleadings and to construe them in the light most favorable to the nonmoving party. *Id.* A factual attack is a challenge to the factual existence of subject matter jurisdiction. *Gen. Ret. Sys. of City of Detroit v. Snyder*, 822 F. Supp. 2d 686, 693 (E.D. Mich. 2011). There is no presumption of truthfulness as to Plaintiffs' complaint and "the court is free to weigh the evidence

and satisfy itself as to the existence of its power to hear the case." *Id*. (quoting *Ritchie*, 15 F.3d at 598. The burden remains with Plaintiffs to establish that jurisdiction exists. *Shepherd v. Cancer & Hematology Centers of W. Michigan*, P.C., No. 1:22-CV-734, 2023 WL 4056342, at *5 (W.D. Mich. Feb. 28, 2023) (citing *Rogers v. Stratton Indus. Inc.*, 798 F.2d 913, 915 (6th Cir. 1986) (per curiam)).

In reviewing a 12(b)(6) motion, the Court "accept[s] all of the complaint's factual allegations as true and determine[s] whether these facts sufficiently state a plausible claim for relief." *Fouts v. Warren City Council*, 97 F.4th 459, 464 (6th Cir. 2024) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007)). The Court "must 'construe the complaint in the light most favorable to the plaintiff, accept all well-pleaded factual allegations as true, and examine whether the complaint contains sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.'" *Norris v. Stanley*, 73 F.4th 431, 435 (6th Cir. 2023) (citations and internal quotation marks omitted). Facial plausibility requires a plaintiff to "plead[] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted).

III.

Flagstar moves to dismiss Plaintiffs' complaint for failure to establish Article III standing and failure to state a claim as to any of their eighteen counts. *See*

generally ECF No. 58. The Court is bound to consider the standing question first "since the Rule 12(b)(6) challenge becomes moot if this court lacks subject matter jurisdiction."[3] *Gen. Ret. Sys. of City of Detroit v. Snyder*, 822 F. Supp. 2d 686, 693 (E.D. Mich. 2011) (quoting *Moir v. Greater Cleveland Regional Transit Authority*, 895 F.2d 266, 269 (6th Cir.1990). The Plaintiff bears the burden of proving subject matter jurisdiction to survive dismissal. *Gen. Ret. Sys.*, 822 F. Supp. 2d at 693.

A. PLAINTIFFS HAVE ARTICLE III STANDING AS TO FUTURE HARM

To establish standing, a plaintiff must satisfy three elements: (1) the plaintiff must have suffered an injury that is "(a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical"; (2) there must be a causal connection between the injury and the conduct complained of such that it is "fairly traceable to the challenged action of the defendant"; (3) it must be likely that the injury will be redressed by a favorable decision. *Carman v. Yellen*, 112 F.4th 386 (6th Cir. 2024).

Flagstar argues that Plaintiffs lack standing because they allege injuries that are not cognizable; they do not sufficiently allege that the breach was traceable to Flagstar; extrinsic evidence forecloses the possibility that any Plaintiffs have suffered (or will suffer) an injury because of the breach and that the injuries they allege are traceable to Flagstar; and Plaintiffs have not produced any evidence to

[3] Standing goes to a court's subject matter jurisdiction. *Myslivecek v. FCA US LLC*, No. 21-10346, 2022 WL 17904526 (E.D. Mich. Dec. 23, 2022).

support they have met the injury or causal connection prongs of standing. *See generally* ECF No. 58. These challenges are both facial and factual attacks on Plaintiffs' standing. The Court will address both sets of challenges.

1. Flagstar's Facial Attacks on Plaintiffs' Standing Fail

"A facial attack on the subject-matter jurisdiction alleged in the complaint questions merely the sufficiency of the pleading." *Enriquez-Perdomo v. Newman*, 54 F.4th 855, 861 (6th Cir. 2022). When considering a facial attack, the Court will "take the allegations in the complaint as true" and assess whether those allegations establish jurisdiction. *Id.* Here, Flagstar claims Plaintiffs insufficiently pleaded as to injury and causal connection. ECF No. 58, PageID.696-699, 701-709. The Court disagrees.

i. *Plaintiffs Have Sufficiently Pleaded Cognizable Injuries*

Plaintiffs alleged the following injuries in their complaint: (1) misuse of their PII via fraud and identity theft; (2) the time, effort, and mitigation costs associated with having their PII compromised in a data breach (i.e., the costs associated with being subjected to future harm)[4]; (3) an increase in phishing spam calls, text messages, and physical mail; (4) lost value of their PII; (5) loss of privacy; and (6)

[4] For example: Plaintiff Smith alleges having to "continue[] to spend time and effort researching the breach and monitoring his accounts for fraudulent activity." ECF No. 52, PageID.548; Plaintiff Kennedy alleges needing to "continue paying for [credit monitoring] services indefinitely to monitor his accounts and attempt to mitigate against harm." *Id.* at PageID.549; and Plaintiff Turner "froze his credit accounts" and "purchased temporary monitoring and identity theft protection." *Id.* at PageID.555.

overpayment and loss of benefit of the bargain. ECF No. 52, PageID.548-556. As to the actual alleged misuses of their PII, Flagstar does not contest that these are cognizable injuries, nor does Flagstar argue that Plaintiffs have not plead enough to survive a facial attack as to these injuries. *See* ECF No. 58, PageID.696. Instead, Flagstar argues that Plaintiffs have failed to adequately allege that these injuries are traceable to the Flagstar breach. *Id.* The Court will address that argument in the next section (Section III(A)(1)(ii)), but here agrees that actual misuse of PII resulting in fraud or identity theft is a cognizable injury for the purposes of standing, and that Plaintiffs have sufficiently alleged this injury.

Actual Injuries

As to Plaintiffs' other actual injuries, the Court finds they are cognizable:

Increases in the number of scam and phishing calls, texts, and emails are cognizable injuries. *Tate v. EyeMed Vision Care, LLC*, No. 1:21-CV-36, 2023 WL 6383467, at *5 (S.D. Ohio Sept. 29, 2023); *see also Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023) (likening unsolicited calls and messages to the common law tort of intrusion-upon-seclusion). Plaintiffs have sufficiently alleged this injury. ECF No. 52, PageID.549-551, 554.

Overpayment and loss of benefit of the bargain are cognizable injuries. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447 (D. Md. 2020), *Lochridge v. Quality Temp. Servs., Inc.,* No. 22-CV-12086, 2023 WL

4303577, at *3 (E.D. Mich. June 30, 2023). Where, as here, Plaintiffs allege there was "an explicit or implicit contract for data security based on [defendant's] privacy statements, that they had placed a significant value in data security, and that had they known the truth about [defendant's] data security practices they would have paid less" or not at all, courts have found cognizable injury sufficient for establishing standing. *Marriott*, 440 F. Supp. 3d at 464-66; *see also* ECF No. 52, PageID.612-614, 558-559. The cases relied upon by Flagstar are distinguishable in that plaintiffs in those cases were not alleging some defect in the product or services rendered. *See In re: Cmty. Health Sys., Inc.,* No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016) (finding overpayment injury was not cognizable where plaintiffs alleged a portion of their premium payments to health providers was made for protection of their patient data); *see also In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (same). Here, Plaintiffs have sufficiently alleged injury as to overpayment and loss of benefit of the bargain.

Loss of Privacy is a cognizable injury where the information was viewed by an unauthorized person or publicly disclosed, and a concrete or particularized injury arose from the loss. *See In re Practicefirst Data Breach Litig.,* No. 121CV00790JLSMJR, 2022 WL 354544, at *7-8 (W.D.N.Y. Feb. 2, 2022), report and recommendation adopted, No. 21CV790JLSMJR, 2022 WL 3045319

(W.D.N.Y. Aug. 1, 2022). Here, Plaintiffs have alleged that their information was published on the dark web and due to that publication, they have suffered concrete harm as a result. *See e.g.,* ECF No. 52, PageID.550 ("Mr. Wiedder's PII, including his Security Number, was located on the dark web following the breach. As a result of the breach, Mr. Wiedder has experienced an increase in suspicious phishing spam calls, text messages, and emails following the breach."); *see also id.* at PageID.555 (Mr. Turner alleges his PII was located on the dark web).

Courts are split as to whether loss of value to PII is a cognizable injury for the purposes of standing. *Compare Lochridge,* No. 22-CV-12086, 2023 WL 4303577 (E.D. Mich. June 30, 2023) (holding loss in value of PII does not suffice as an injury sufficient to confer standing absent allegations that plaintiff attempted to sell their PII) *with Marriott,* 440 F. Supp. 3d 447 (D. Md. 2020) (recognizing the loss of value in PII as a cognizable injury even where plaintiffs had not attempted to sell their PII). Flagstar argues that PII has no monetary value for its owners, meaning any loss in value to Plaintiffs' PII is lost only by potential buyers of such PII or those who seek to profit from Plaintiffs' PII. ECF No. 58, PageID.707. Because Plaintiffs have not alleged they "intended to sell their PII but could not, or that they were forced to accept a discounted price" for their PII, Flagstar argues, the loss in value of their PII is not a cognizable injury. *Id; see also Lochridge,* 2023 WL 4303577, at *4. However, this Court is persuaded by Plaintiffs' argument that Plaintiffs' PII has

independent value to them, unrelated to its value on the market. For example, in *Marriott,* the court recognized that "[w]hether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their" PII. *Marriott*, 4440 F. Supp. 3d at 462. The court in *Marriott* found sufficient that plaintiffs had alleged that they had "suffered lower credit scores as a result of the data breach." *Id.* Here, at least one Plaintiff (Plaintiff Nasrallah) alleged his credit score was negatively impacted by fraud resulting from the Data Breach. ECF No. 52, PageID.553. Insofar as members of Plaintiffs' class allege loss in value to their PII in this manner—loss in their ability to avail themselves of the digital economy or parts of the financial sector—the Court finds this is a cognizable injury. As far as Plaintiffs that allege only that their PII lost monetary value, the Court finds this is not a cognizable injury.

Future Harm

Flagstar argues that future harm, standing alone, is not a cognizable injury sufficient to confer standing. ECF No. 58, PageID.701. Its argument relies on the U.S. Supreme Court's decision in *TransUnion LLC v. Ramirez*, where the Court held that certain plaintiffs who had not yet suffered any concrete harms could not establish standing on their risk of future harm alone. 594 U.S. 413, 422-30 (2021). Flagstar also argues that *TransUnion* abrogates *Galaria v. Nationwide Mutual Insurance Company*, a Sixth Circuit case addressing what is required to establish

Article III standing where plaintiffs allege risk of future harm because of a data breach. 663 F. App'x 384 (6th Cir. 2016). The Sixth Circuit has not yet reconsidered *Galaria* in light of *TransUnion*. Because this Court must follow Sixth Circuit precedent, and because the Court is persuaded by the reasoning of other decisions recognizing *Galaria* as good law post-*TransUnion*, the Court will apply *Galaria* here. *See Doe v. Mission Essential Grp., LLC*, No. 2:23-CV-3365, 2024 WL 3877530 (S.D. Ohio Aug. 20, 2024); *Lochridge,* 2023 WL 4303577 (E.D. Mich. June 30, 2023); *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-186-CHB, 2024 WL 1366832 (W.D. Ky. Mar. 29, 2024) (summarizing *TransUnion* and finding that future harm satisfies Article III's standing requirement when plaintiffs can demonstrate (1) that there is substantial risk of future harm or the harm is imminent and (2) whether the harm is concrete, meaning, whether there is both a common law analog and currently felt concrete harms, such as mitigation costs).

Under *Galaria*, to establish a cognizable Article III injury a plaintiff must allege "substantial risk of harm, coupled with reasonably incurred mitigation costs." 663 F. App'x 384, 388 (6th Cir. 2016). Whether the mitigation costs were "reasonably incurred" depends on if the risk is truly substantial and impending. *Doe*, 2024 WL 3877530, at *5. The Court in *Galaria* found that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs'

complaints" and that "it would be unreasonable to expect Plaintiffs to wait for actual misuse. . . before taking steps to ensure their own personal and financial security." *Galaria*, 663 F. App'x at 388. Here, Plaintiffs allege that their PII was targeted and stolen in the Flagstar Data Breach. ECF No. 52, PageID.547-556, 582-583. The Court finds these allegations, coupled with the named Plaintiffs' individual allegations demonstrating mitigation measures they took (*see* ECF No. 52, PageID.548-556), are sufficient to survive a facial attack to standing.

Flagstar argues *Galaria* is distinguishable because the risk associated with a ransomware attack is less substantial than the kind of cyber-attack at issue in *Galaria,* where the cyber attackers "obtain confidential information *for purposes of identity theft*." ECF No. 58, PageID.705 (arguing that ransomware attacks are not for the purpose of identity theft, but rather, to obtain the ransom payment). Flagstar also argues that at least some of the named Plaintiffs' mitigation expenses were unreasonably incurred because their data was *not* compromised in the breach. *Id.* at PageID.691-693. The Court finds that these are factual attacks on whether Plaintiffs can in fact demonstrate that this specific data breach exposes them to substantial risk of future harm and that their mitigation costs were reasonable. Thus, the Court will address those arguments in the factual attack section below.

ii. *Plaintiffs have sufficiently pleaded traceability*

Flagstar also argues that Plaintiffs have failed to adequately allege traceability. ECF No. 58, PageID.696. According to Flagstar, Plaintiffs must allege: "(1) the PII they believe was compromised in the Cyber Incident, (2) when the purported misuse of their PII occurred (including that it even post-dated the incident), or (3) that their PII has not been previously compromised in other security incidents." *Id*.

In general, "the traceability requirement mainly serves to eliminate those cases in which a third party and not a party before the court causes the injury." *Galaria*, 663 F. App'x at 390. The Sixth Circuit in *Galaria* found that injuries resulting from PII lost in a data breach are fairly traceable to the defendant's failure to provide sufficient safeguards against hackers. *Id.* ("Although hackers are the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because [defendant] allegedly failed to secure the sensitive personal information entrusted to its custody.").

Intuitively, the existence of a data breach, standing alone, cannot confer traceability to a defendant. *Sifuentes v. Dave Inc*., No. 1:23-CV-984, 2023 WL 7295187 (W.D. Mich. Nov. 6, 2023). A plaintiff must also allege that their data was compromised in the breach. *See, e.g, Tate*, 2023 WL 6383467, at *5 (holding that an increase in spam calls was traceable to the data breach where plaintiff's email account was hacked by cyber attackers who "presumably sought to profit from cyber

attack," and this created a "reasonable inference" that data breach led to the pleaded injury); *Doe*, 2024 WL 3877530 at *7 (holding that "[a]mong other failures, he does not allege that his email address was accessed during the Data Incident" when the alleged injury was an increase in targeted spam emails).

Thus, the Court finds Plaintiffs who cannot allege that their information was compromised in the data breach have not sufficiently pleaded traceability. Here, although Flagstar denies that certain Plaintiffs had PII compromised in the data breach that logically relates to the injuries they allege (e.g., Plaintiff Silva alleges that he experienced multiple unauthorized withdrawals from his banking cards, but his bank card information was not compromised in the breach) and denies that certain Plaintiffs' PII were implicated at all (e.g., "[N]o personal information associated with Plaintiff Tallman or Plaintiff McCarthy was compromised during the Cyber Incident"), all Plaintiffs have alleged that they were "notified by Flagstar that [their] PII was compromised in the Data Breach." ECF No. 52, PageID.548-556.[5] The Court finds this is sufficient to survive a facial attack to standing. *Cf. Shepherd v. Cancer & Hematology Centers of W. Michigan, P.C.*, No. 1:22-CV-734, 2023 WL 4056342, at *6 (W.D. Mich. Feb. 28, 2023) (holding plaintiff could not

[5] Plaintiff McCarthy alleges he was "notified by a third-party monitoring company that his PII was compromised in the Data Breach." ECF No. 52, PageID.551. Despite not being notified by Defendant Flagstar specifically, the Court finds this sufficient for the purposes of pleading traceability.

establish standing where she could not refute *factual* declaration that none of her PII had been accessed during the breach).

2. Flagstar's Factual Attacks as to Plaintiffs' Standing Fail as to Future Harm and Succeed as to All Other Injuries

Flagstar has presented evidence to undermine Plaintiffs' ability to establish standing. In so doing, Flagstar initiates a factual attack on Plaintiffs' standing. A factual attack is a challenge to the factual existence of subject matter jurisdiction. *Gen. Ret. Sys.*, 822 F. Supp. 2d at 693. There is no presumption of truthfulness as to Plaintiffs' complaint and "the court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case." *Id.* at 693 (quoting *United States v. Ritchie*, 15 F.3d 592, 598 (6th Cir.1994)). The burden remains with Plaintiffs to establish that jurisdiction exists. *Shepherd,* 2023 WL 4056342, at *5 (citing *Rogers v. Stratton Indus. Inc.*, 798 F.2d 913, 915 (6th Cir. 1986) (per curiam)).

Plaintiffs argue that the Court "should engage in a factual inquiry regarding the complaint's allegations only when the facts necessary to sustain jurisdiction do not implicate the merits of the plaintiff's claim." ECF No. 72, PageID.1513 (quoting *Gentek Bldg. Prod., Inc. v. Sherwin-Williams Co.*, 491 F.3d 320, 330-31 (6th Cir. 2007)). Here, Plaintiffs argue that because the traceability inquiry implicates the causation element of Plaintiffs' tort and statutory claims, the Court should "find that jurisdiction exists and consider the objection a direct attack on the merits of the

plaintiff's claim." ECF No. 72, PageID.1513-1514 (quoting *Genteck*, 491 F.3d at 330-31).

However, the question of subject matter jurisdiction and the merits will "normally be considered intertwined where the *same statute* provides both the basis of federal court subject matter jurisdiction and the cause of action." *Moore v. Lafayette Life Ins. Co.*, 458 F.3d 416, 444 (6th Cir. 2006) (emphasis added). This Court has held that the intertwinement rule does not apply when the "factual dispute does not go to an element of a federal statute providing the court with jurisdiction." *Myslivecek v. FCA US LLC*, No. 21-10346, 2022 WL 17904526, at *6-7 (E.D. Mich. Dec. 23, 2022) (holding the intertwinement rule did not apply because plaintiffs' underlying claims were "all state law claims, and the Class Action Fairness Act [was] the basis for the court's jurisdiction"). The Court finds the intertwinement rule from *Genteck* does not apply here because the basis for this court's jurisdiction is the Class Action Fairness Act and not any of Plaintiffs' common law or statutory claims. ECF No. 52, PageID.545. Thus, the Court will consider Flagstar's factual attack.

As evidence that Plaintiffs lack standing to pursue their claims, Flagstar presents: a declaration from Jennifer Charters (ECF No. 58-2); a declaration from William Hardin (ECF No. 60); and a "Statement of Work" from the security vendor

it worked with after the breach to, among other things, monitor the dark web for Plaintiffs' PII (ECF No. 75-4).

As a preliminary matter, Plaintiffs challenge this Court's ability to rely on the Declaration of Jennifer Charters. In reviewing evidence presented on a factual challenge to standing, the Court "has broad discretion with respect to what evidence to consider in deciding whether subject matter jurisdiction exists, including evidence outside of the pleadings, and has the power to weigh the evidence and determine the effect of that evidence on the court's authority to hear the case." *Shepherd*, 2023 WL 4056342, at *4 (quoting *Ohio Nat. Life Ins. Co. v. United States*, 922 F.2d 320 (6th Cir. 1990). As the court in *Shepherd* held, where the "Plaintiff has given the Court no reason to doubt the authenticity of [declarant's] declaration, nor has she raised any argument that the declaration contains false assertions" the Court may rely on the evidence in the declaration when evaluating whether it has jurisdiction. *Shepherd*, 2023 WL 4056342, at *5. Here, Plaintiffs allege the declaration is faulty because it was not prepared by Ms. Charters and that the "declaration reflects what she learned secondhand at executive meetings . . ." ECF No. 71, PageID.1207. However, these allegations do not give the Court reason to doubt the authenticity of the declaration. Ms. Charters' declaration was based on her firsthand knowledge as an executive during the Data Breach, and Plaintiffs do not contest this. *See id.* ([Ms. Charters] has no *relevant* firsthand knowledge of the matters discussed in her

declaration") (emphasis added)). The Court may consider this evidence when determining standing.

i. Plaintiffs Cannot Survive Flagstar's Factual Attack as To Their Actual Harms

Flagstar argues that extrinsic evidence "confirms" that Plaintiffs cannot prove their injuries in fact, nor can they connect their injuries to the breach. ECF No. 58, PageID.699.

First, Flagstar offers evidence that Plaintiffs' PII was never on the dark web: both Flagstar's cybersecurity vendor, Kroll, and a cybersecurity expert Flagstar hired, William Hardin from CRA International, Inc., monitored the dark web and found none of the compromised Flagstar data. ECF No. 58-2, PageID.741-742 ("Flagstar engaged Kroll Associates, Inc. to conduct . . . daily monitoring of the dark web . . . and identified no evidence that the threat actor released any Flagstar data[.]"); ECF No. 58-3, PageID.752 (William Hardin opining that the threat actor "kept to the agreement and did not post, sell, or otherwise make available Flagstar's data" from the breach."). Next, Flagstar provides evidence that Plaintiffs' PII was compromised and exposed in other breaches. For example, Ms. Charters confirmed in her declaration that Plaintiffs Smith, Kennedy, Wiedder, Hernandez, Nasrallah, Silva, and Turner all had PII compromised in the Accellion breach. ECF No. 58-2, PageID.743. Lastly, Flagstar provided evidence that some of the injuries claimed by Plaintiffs cannot be traceable to the Flagstar Data Breach because the PII that

could have caused those injuries was not compromised in the breach. *See e.g.,* ECF No. 58-2, PageID.742 ("Plaintiff Silva's banking card information was not exfiltrated in the Cyber Incident."), ECF No. 52, PageID.553 ("Mr. Silva has suffered identity theft and fraud in the form of multiple unauthorized withdrawals from his banking cards."). Notably, some Plaintiffs had no PII compromised in the breach at all. ECF No. 58-2, PageID.742 ("No personal information associated with Erin Tallman or Michael McCarthy was exfiltrated during the Cyber Incident.").

Flagstar also relies on the fact that in exchange for the ransom it paid, it was allowed to "completely delet[e] all data acquired by the threat actor from Flagstar's network." ECF No. 58-2, PageID.741. Flagstar claims it received guarantees from the threat actor that "there were no other copies of the data in the possession of anyone outside of Flagstar." *Id.*

Plaintiffs, in response, attack the sufficiency of the evidence Flagstar presents. *See generally* ECF No. 72. For example, Plaintiffs point out that Mr. Hardin and Kroll only conducted dark web searches beginning in October 2022—ten months after the breach had occurred. ECF No. 72, PageID.1499; *see also* ECF No. 72-6, PageID.1704-1707. They also point out that Mr. Hardin conceded in his deposition that, had Plaintiffs' information been published and deleted on the dark web before he conducted his search, it would not have shown up in his monitoring. ECF No. 72, PageID.1499-1500. Plaintiffs also question the thoroughness of his search—

pointing out that Mr. Hardin only searched a "small fraction of an unlimited, unknown number of sites on the dark web." ECF No. 72, PageID.1500. And Plaintiffs undermine the credibility of Ms. Charters by accusing her of lacking personal knowledge on the topics in her declaration. *See, e.g.*, ECF No. 72, PageID.1490.

Plaintiffs also provide the Court with the email exchanges from the ransom negotiations. *See* ECF No. 72-5. These emails, Plaintiffs argue, demonstrate that the cyber attackers are untrustworthy and that the ransom agreement should be no guarantee that the criminals followed through on their promises to delete and retain no copies of Plaintiffs' PII. *See* ECF No. 72-5.

Although Plaintiffs have raised valid challenges to Flagstar's contention that the evidence undoubtedly "confirms" that Plaintiffs' PII was never published on the dark web, Plaintiffs have offered *no affirmative evidence* to support that it was. Without more, Plaintiffs are asking this Court to rely on the factual allegations in their complaint alone; but "[i]n a factual attack, the allegations in the complaint are not afforded a presumption of truthfulness. . . " *Shepherd*, 2023 WL 4056342, at *2. Instead, "the court weighs competing evidence to determine whether subject matter jurisdiction exists" and without pointing to any evidence of their own, the Court finds Plaintiffs cannot meet their burden. *Id.; see also De Angelis v. Nat'l Ent. Grp., LLC*, No. 2:17-CV-924, 2018 WL 11316612, at *6 (S.D. Ohio July 25, 2018)

("Because the question [is] a factual issue, [plaintiff] cannot meet her burden of proving standing without pointing to any evidence of her own.").[6]

Because Plaintiffs McCarthy and Tallman, similarly, have not put forth any evidence to refute Flagstar's evidence that they had *no* PII compromised during the breach, the Court summarily dismisses them from this action. *See* ECF No. 58-2, PageID.742.

ii. Plaintiffs Can Meet Their Burden as to Future Harm

The risk of future harm associated with a data breach is merely "speculative" where the hacker has no intention to misuse the information. In fact, courts have regularly recognized that existence of a data breach alone is not sufficient to demonstrate risk of future harm. *See Reilly*, 664 F.3d 38 (3d Cir. 2011).

Under *Galaria*, the Sixth Circuit held it was reasonable to assume plaintiffs were at risk of future harm, sufficient to confer standing, where the PII had been specifically targeted and plaintiffs' data was in the hands of the cyber attacker. *Galaria*, 663 F. App'x at 388. This is consistent with other courts that look to the intent of the breach when deciding whether the risk of exposure is sufficiently imminent to confer standing. *See Savidge*, 2024 WL 1366832 (W.D. Ky. Mar. 29, 2024); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152-53 (3d Cir. 2022).

[6] The Court finds persuasive that Plaintiffs have been able to engage in months-long discovery and still have not presented any information demonstrating that their PII was on the dark web.

Flagstar offers evidence in an attempt to distinguish the Data Breach from the breach in *Galaria*. For one: the fact that this was a ransomware attack. According to William Hardin, payment of a ransom generally ensures that data will not be posted on the dark web. *See* ECF No. 75-5, PageID.1813-1814; *see also id*. at PageID.1811 ("I'm saying that based off numerous amount of ransoms that I have handled and payments that I have made that threat actors out there abide by the pirate code that they do not publicize the information [when ransom is paid]."). Flagstar also heavily rests its argument on the fact that it deleted the PII off of the cyber attackers' server. ECF No. 58, PageID.693 ("While Plaintiffs allege on 'information and belief' that the PII compromised in the Cyber Incident was 'made available to other criminals on the dark web,' that allegation is flatly wrong. In fact, the stolen data was deleted by Flagstar and was never released or posted on the dark web.") (quoting ECF No. 52, PageID.547).

However, the emails Plaintiffs present from the ransom negotiations are sufficient to demonstrate the risk that the cyber attackers intend to use Plaintiffs PII in the future. *See* ECF No. 72-5. The Court finds these emails persuasive to demonstrate that there is risk of future harm sufficient to confer standing on Plaintiffs.

The Court notes that the fact that it has been 3 years since the breach undermines that Plaintiffs' future harm is "imminent," however, given the weight of

all the evidence, the Court finds Plaintiffs have met their burden to survive Flagstar's factual attack to standing. *Savidge,* 2024 WL 1366832, at *17) ("when the stolen data includes certain high-risk information . . . the risk of identity theft remains, even as time passes.").

B. PLAINTIFFS FAIL TO STATE A CLAIM AS TO ALL COUNTS WITH THE EXCEPTION OF COUNT IX

1. Common Law Claims

Applying Michigan's choice-of-law rules, the Court finds that Michigan law applies to Plaintiffs' tort and contract claims. *Hummel v. Teijin Auto. Techs., Inc.*, No. 23-CV-10341, 2023 WL 6149059, at *3 (E.D. Mich. Sept. 20, 2023) ("[A] federal court . . . must apply the choice-of-law rules of the forum state.") (finding Michigan tort and contracts law applied in a comparable data breach case).

i. *Negligence*[7] (Count I)

To state a claim for negligence, Plaintiffs must establish that "(1) the defendant owed the plaintiff a legal duty, (2) the defendant breached the legal duty, (3) the plaintiff suffered damages, and (4) the defendant's breach was a proximate cause of the plaintiff's damages." *Hummel*, 2023 WL 6149059, at *5 (quoting *Hill v. Sears, Roebuck & Co.*, 492 Mich. 651, 660 (2012)). "Companies have a duty to

[7] Because "negligence *per se* is not an independent cause of action" and the Court finds Plaintiffs' allegations as to their Negligence claim insufficient to survive a motion to dismiss because they fail as to the harm element, the Court summarily dismisses Count II of Plaintiffs' complaint. *Abnet v. Coca-Cola Co.*, 786 F. Supp. 2d 1341, 1345 (W.D. Mich. 2011).

take reasonable precautions" to protect users' PII "due to the reasonably foreseeable risk of danger of a data breach incident." *Lochridge*, 2023 WL 4303577, at *6 (E.D. Mich. June 30, 2023) (internal quotations omitted). The Court finds Flagstar also has this duty.

Here, Plaintiffs allege that Flagstar breached that duty by failing to: "(a) exercise reasonable care and implement adequate security (b) detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and the Class Members' PII in Flagstar's possession had been or was reasonably believed to have been, stolen or compromised." ECF No. 52, PageID.598.

Despite the information asymmetry as to what Flagstar did to secure Plaintiffs' PII, this Court has found that more than a mere recitation of industry standards and conclusory statements is necessary to survive a motion to dismiss. *Hummel*, 2023 WL 6149059, at *6-7 (holding that Plaintiffs' allegation—that defendant could have prevented the breach by securing and encrypting the folders containing plaintiffs' PII—was sufficient to survive a motion to dismiss). Here, Plaintiffs also specifically allege failure to encrypt their PII as a reason for the

breach. *See, e.g.*, ECF No. 52, PageID.578, 639. The Court finds this is a sufficiently alleged breach to survive a motion to dismiss.

The Court also finds, as to the causation element of a negligence claim, that Plaintiffs' have sufficiently alleged facts necessary to survive a motion to dismiss for the reasons set out in the Court's discussion of traceability under Section III(A)(2)(ii). *Hummel*, 2023 WL 6149059, at *12 ("if allegations . . . satisfy Article III traceability, then Defendant, not a third party, must have caused Plaintiff's injuries. While not dispositive, this goes a long way towards Plaintiff showing that her injuries were proximately caused by Defendant.").

However, the Court finds Plaintiffs fail to allege cognizable injury under Michigan law, and thus, fail to state a claim. *Lochridge*, 2023 WL 4303577, at *6 ("Michigan law has recognized that 'damages 'incurred in anticipation of possible future injury rather than in response to present injuries,' are not cognizable under Michigan law" for negligence or breach of contract) (citing *Doe v. Henry Ford Health Sys.*, 308 Mich. App. 592, 600 (2014)).

Thus, the Court grants Flagstar's Motion to Dismiss as to Count I.

ii. *Unjust Enrichment* (Count III)

To state a claim for Unjust Enrichment under Michigan law, a plaintiff must demonstrate "(1) the receipt of a benefit by the defendant from the plaintiff and (2) an inequity resulting to the plaintiff because of the retention of the benefit by the

defendant." *Lochridge*, 2023 WL 4303577, at *6. That benefit must come "directly from the plaintiff." *Id*. at *7. Mere monetary benefits derived from the "use of Plaintiffs' [PII]" is not sufficiently direct from the Plaintiffs to satisfy the first prong of an Unjust Enrichment claim. *Id*.

Here, Plaintiffs allege Flagstar was unjustly enriched by "the conferral upon it of the PII pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information." ECF No. 52, PageID.604. The Court finds this is insufficient to satisfy the directness requirement and therefore grants Flagstar's motion to dismiss as to Count III.

iii. *Breach of Confidence* (Count IV)

A breach of confidence claim involves "the unconsented, unprivileged *disclosure* to a third party of nonpublic information that the defendant has learned within a confidential relationship." *Eickenroth v. Roosen, Varchetti & Olivier*, PLLC, No. 20-11647, 2021 WL 1224912, at *4 (E.D. Mich. Mar. 31, 2021) (emphasis added).

Plaintiffs argue that the disclosure need not be intentional, but by Flagstar "knowingly allowing" the unauthorized disclosure of their PII by the cyber attackers, they can be held liable for breach of confidence. ECF No. 72, PageID.1522. The Court disagrees. Disclosure is defined as "[t]o make (something) known or public." Black's Law Dictionary (12th ed. 2024). Plaintiffs fail to allege any facts

demonstrating that Flagstar did anything to make their PII known to the public. The actors "making" their PII known to the public are the cyber attackers, not Flagstar. *See Foster v. Health Recovery Servs., Inc.*, 493 F. Supp. 3d 622, 636 (S.D. Ohio 2020) (holding no claim for Breach of Confidence where *Defendant* did not commit an intentional or unintentional act of disclosure). Because Plaintiffs fail to allege facts demonstrating that Flagstar disclosed Plaintiffs' confidential information, the Court grants Flagstar's motion to dismiss Count IV.

iv. *Invasion of Privacy – Intrusion Upon Seclusion* (Count V)

The three elements establishing Invasion of Privacy by intrusion upon seclusion are: "(1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man." *Green v. Lansing Automakers Fed. Credit Union*, No. 342373, 2019 WL 3812108, at *5 (Mich. Ct. App. Aug. 13, 2019). Michigan courts recognize that the objectionable obtaining of the information must be done by the defendant that the plaintiffs are suing. *See Meier v. Detroit Diesel Corp.*, No. 268009, 2006 WL 2089208, at *3 (Mich. Ct. App. July 27, 2006); *Szappan v. Meder*, No. 18-12244, 2020 WL 209746 (E.D. Mich. Jan. 14, 2020).

Plaintiffs do not allege any facts showing that Flagstar obtained their PII via an objectionable method. In fact, Plaintiffs concede they provided their PII to

Flagstar willing, in order to utilize Flagstar's services. ECF No. 52, PageID.558; ECF No. 72, PageID.1525. Thus, the Court finds Plaintiffs have not stated a claim for Invasion of Privacy and grants Flagstar's motion to dismiss as to Count V.

v. *Breach of Express Contract* (Count VI)

To state a claim for Breach of Contract, a plaintiff must allege facts sufficient to show: "(1) there was a contract, (2) the other party breached the contract, and (3) this breach resulted in damages to the party claiming breach." *Johnson v. Westfield Ins. Co*., No. 19-11213, 2019 WL 3456808, at *2 (E.D. Mich. July 31, 2019) (citing *Miller-Davis Co. v. Ahrens Const., Inc*., 495 Mich. 161, 178 (2014)).

Here, Plaintiffs allege that Flagstar's Privacy Policy is the express agreement between the parties. ECF No. 52, PageID.612. But courts have held, and this Court agrees, that such privacy notices are "not contractual in nature." *Tucker v. Marietta Area Health Care, Inc*., No. 2:22-CV-184, 2023 WL 423504, at *5 (S.D. Ohio Jan. 26, 2023). Rather, these notices "serve to inform [consumers] of their rights under federal law." *Id.* The Court finds this is true of Flagstar's privacy policy and therefore finds Plaintiffs fail to state a Breach of Express Contract claim. The Court grants Flagstar's motion to dismiss as to Count VI.

vi. *Breach of Implied Contract* (Count VII)

The elements to state a claim for an implied contract are the same three necessary elements of stating an express contract claim. *See supra* (v), p. 32. An

implied contract "may arise from [the parties'] conduct, language, or other circumstances evidencing their intent to contract." *Lochridge*, 2023 WL 4303577, at *7 (citing *Featherston v. Steinhoff*, 226 Mich. App. 584 (1997)). An implied contract must still "satisfy the elements of mutual assent and consideration." *Hummel*, 2023 WL 6149059, at *8 (quoting *Mallory v. City of Detroit*, 181 Mich. App. 121, 127 (1989)). Flagstar, here, contest Plaintiffs' ability to adequately allege mutual assent and breach. *See* ECF No. 58, PageID.720-722.

Courts find mutual assent obvious in situations similar to what Plaintiffs allege here. As the court in *Hummel* articulated: "it is incredibly difficult to imagine, how, in our day and age of data and identity theft, the mandatory receipt of PII would not imply the recipient's assent to protect the information sufficiently." 2023 WL 6149059, at *11 (quoting *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016)) (internal quotations omitted). And perhaps more intuitively, the court held: "When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected." *Id.* at *10 (quoting *Castillo*, 2016 WL 9280242, at *9). Thus, the Court finds Plaintiffs' adequately allege mutual assent for giving their PII in exchange for Flagstar's services and an implied assurance that the PII would be sufficiently protected.

As for breach, Plaintiffs allege Flagstar breached this implied contract when it "failed to take reasonable steps to use safe and secure systems to protect that information." ECF No. 52, PageID.616. This court has previously found similar allegations sufficient to state a claim for breach of implied contract. *See Lochridge*, 2023 WL 4303577, at *7.

However, as mentioned above, future harm is not a cognizable injury under Michigan law for breach of contract. *Doe*, 308 Mich. App. at 602. Thus, the Court finds Plaintiffs have failed to adequately state their Breach of Implied Contract claim; and the Court grants Flagstar's motion to dismiss Count VII.[8]

vii. *Declaratory Judgment* (Count VIII)

Plaintiffs justify their declaratory judgment claim by alleging they "continue to suffer injury as a result of the compromise of their PII and *remain at imminent risk that further compromises of their PII will occur in the future* . . ." ECF No. 52, PageID.618. This Court has held a plaintiff may not seek declaratory and injunctive relief designed to prevent future breach. *See Lochridge*, 2023 WL 4303577, at *8 ("Plaintiff may have alleged a sufficient risk of future identity theft as a result of the previous data breach, he has not alleged any facts tending to show that a second data

[8] The Court is not persuaded by Flagstar's argument that the implied contract is unenforceable by the statute of frauds. *Considine v. Always Christmas*, No. 184801, 1997 WL 33344951 (Mich. Ct. App. Aug. 22, 1997) (holding the statute of frauds does not apply to contracts of indefinite periods).

breach is currently impending or there is a substantial risk that one will occur."). The Court finds Plaintiffs have failed to state a claim for declaratory judgment and grants Flagstar's motion to dismiss as to Count VIII.

2. Statutory Claims

i. *California Consumer Privacy Act ("CCPA")* (Count IX)

The CCPA permits "any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." Cal. Civ. Code § 1798.150(a)(1). Flagstar argues that Plaintiffs fail to state a claim under the CCPA because (1) Plaintiffs' allegations are "threadbare recitals of the elements of a cause of action that fall short of stating a claim." ECF No. 58, PageID.724; and (2) Plaintiffs have failed to follow the CCPA's pre-suit notice requirement. *Id.* at PageID.725. The Court finds both of these arguments unpersuasive.

As to Flagstar's first argument, courts have found allegations that are very similar to what Plaintiffs allege here as sufficient to state a claim. *See, e.g., Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, 2021 WL 6882377, at *8 (N.D. Cal. May 6, 2021) (finding Plaintiffs stated a claim by alleging that defendants "allow[ed] unauthorized users to view, use, manipulate, exfiltrate, and steal the

nonencrypted and nonredacted personal information of Plaintiffs and other customers, including their personal and financial information.").

And the Court agrees. *See* ECF No. 52, PageID.620 ("Flagstar violated . . . the CCPA by failing to prevent Plaintiffs' and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Flagstar's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."); *Id.* at ECF No. 52, PageID.578 ("Flagstar was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers, including the need to encrypt customer data on their computer networks, but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring.").

Further, as to Flagstar's notice argument, the Court agrees with Plaintiffs that they need only provide sufficient notice before the *operative* complaint. *Gregorio v. Ford Motor Co.*, 522 F. Supp. 3d 264 (E.D. Mich. 2021). Here, the operative complaint is Plaintiff's Consolidated Class Action Complaint, filed on June 23, 2023. ECF No. 52. Two California plaintiffs, Plaintiffs Wiedder and Smith, mailed notice to Flagstar on June 28, 2022 and June 30, 2022. ECF No. 58, PageID.725. This is more than a year before the Consolidated Class Action Complaint was filed. The purpose of the notice requirement in the CCPA is to give the defendant an

opportunity to cure; the Court finds Flagstar has had such an opportunity and cannot now use the statutory notice requirement to justify dismissal of this claim. *Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 99 Cal. Rptr. 3d 768 (2009). Thus, the Court denies Flagstar's motion to dismiss as to Count IX.

ii. *California Customer Records Act ("CCRA"), Cal. Civ. Code §§ 1798.80, et seq.*, (Count X) and *Washington Data Breach Notice Act ("WDBNA"), Wash. Rev. Code Ann. § 19.255.010* (West), (Count XVII)

Both the CCRA and the WDBNA require businesses that "own or license computerized data that includes PII" to notify the PII's owners if it has been acquired, or reasonably believed to have been acquired, in a security breach. Cal. Civ. Code § 1798.82; Wash. Rev. Code § 19.255.010(8). Under both statutes, notice should be made without unreasonable delay. *Id.*

Flagstar argues that Plaintiffs fail to state a claim under the California Consumer Privacy Act because they fail to allege "actual damages flowing from the delay (and not just the intrusion itself)" and they fail to allege that the delay in disclosure was unreasonable. ECF No. 58, PageID.727. The Court finds it unnecessary to address Flagstar's second argument because the Court agrees that Plaintiffs fail to state a claim under Flagstar's first argument.

When plaintiffs cannot allege injury *resulting from* the delayed notification—as opposed to injury arising from the breach itself—courts dismiss these claims. *See In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.,* 613 F. Supp. 3d

1284, 1300 (S.D. Cal. 2020); *Grigsby v. Valve Corp.,* No. C12-0553JLR, 2013 WL 12310666 (W.D. Wash. Mar. 18, 2013). Here, Plaintiffs from California and Washington all merely allege that they could have "taken steps to protect against fraud and identity theft sooner" had they been more timely notified of the breach. ECF No. 72, PageID.1531. But that argument is without merit where no California or Washington Plaintiff can allege concrete fraud or identity that could have been prevented had the notification of the breach come sooner. *See* ECF No. 52, PageID.548-551, 555-556. Only one Plaintiff, Plaintiff Smith, can even allege attempted unauthorized bank transfers, but *attempted* transfers are not cognizable injuries. *See Whalen v. Michaels Stores, Inc.,* 689 F. App'x 89 (2d Cir. 2017). The Court finds Plaintiffs fail to state a claim and therefore dismisses Counts X and XVII of Plaintiffs' Complaint.

iii. *Colorado Security Breach Notification Act*, Colo. Rev. Stat. §§ 6-1-716, et seq., (Count XIII) and *Colorado Consumer Protection Act*, Colo. Rev. Stat. §§ 6-1-101, et seq. (Count XIV)

Because the only Plaintiff that has standing to sue as to the Colorado state statutes, Michael McCarthy, did not have any data compromised in the breach, the Court dismisses these Counts. *Norman*, 696 F. Supp. 3d 359 (dismissing claims for which there were no named Plaintiffs residing in those states to assert standing as to those state laws); ECF No. 58, PageID.692.

iv. *California Unfair Competition Act ("ULC")*, *Cal. Bus. & Prof. Code §§ 17200, et seq.* (Count XI), *California Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, et seq.* (Count XII), *Indiana Deceptive Consumer Sales Act ("IDCSA"), Ind. Code § 24-5-0.5* (Count XV), *Michigan Consumer Protection Act ("MCPA"), Mich. Comp. Laws Ann. § 445.901 et seq.* (Count XVI), *Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code §§ 19.86.020, et seq.* (Count XVIII)

Both Flagstar in its Motion to Dismiss (ECF No. 58) and Plaintiffs in their responsive brief (ECF No. 72) address these counts together, so the Court will do the same. *See* ECF No. 58, PageID.729-736; ECF No. 72, PageID.1531-1537.

Flagstar argues that Plaintiffs fail to allege cognizable injuries under each of these statutes and because they fail to demonstrate the injury or loss was caused by the Flagstar breach. ECF No. 58, PageID.730.

Each of Plaintiffs' claims has a causation or reliance element. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 804 (N.D. Cal. 2019) (holding to pursue a ULC claim, plaintiffs must show "that they lost money or property *because of* [defendant's] conduct"); *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 641, 200 P.3d 295, 299 (2009) ("Any consumer who suffers any damage *as a result of* the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action" under the CLRA."); *IUE-CWA Loc. 901 v. Spark Energy, LLC*, 440 F. Supp. 3d 969, 976 (N.D. Ind. 2020) ("'A person relying upon an uncured or incurable deceptive act may bring

an action' under the IDSCA.") (citing Ind. Code § 24-5-0.5-4); *Brownlow v. McCall Enterprises, Inc.*, 315 Mich. App. 103, 888 N.W.2d 295 (2016); *Gray v. Amazon.com, Inc.*, 653 F. Supp. 3d 847, 859 (W.D. Wash. 2023), aff'd, No. 23-35377, 2024 WL 2206454 (9th Cir. May 16, 2024)).

Meaning, each Plaintiff must be able to allege facts connecting their alleged injuries to the unlawful, unfair, deceptive, or fraudulent actions of Flagstar. However, the Court has already found that Plaintiffs are unable to trace their actual harms to Flagstar or the breach. *See supra* Section III(A)(2)(i)[9]; *see also Galaria*, 663 F. App'x 384 (implicitly recognizing that the "fairly traceable" requirement is a lower hurdle to clear than causation). Thus, because Plaintiffs cannot allege causation, Plaintiffs are unable to state a claim as to any of their actual harms.

Moreover, Plaintiffs' only remaining injury for which they can adequately plead causation—namely, their risk of future harm and mitigation costs—is not cognizable under these statutes. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012) ("Plaintiffs' allegations that the heightened risk of identity theft, time and money spent on mitigation of that

[9] Similar to the Court's ability during a factual attack to subject matter jurisdiction, "[i]n reviewing a motion to dismiss, the court may consider 'any exhibits attached [to the complaint], public records, items appearing in the record of the case and exhibits attached to defendant's motion to dismiss so long as they are referred to in the Complaint and are central to the claims contained therein.'"). *Geomatrix, LLC v. NSF Int'l*, 629 F. Supp. 3d 691, 700 (E.D. Mich. 2022), aff'd, 82 F.4th 466 (6th Cir. 2023) (quoting *Bassett v. NCAA*, 528 F.3d 426, 430 (6th Cir. 2008)). Thus, the Court finds it may consider the extrinsic evidence attached to Flagstar's Motion to Dismiss here.

risk, and property value in one's information, do not suffice as injury under the UCL, FAL, and/or the CLRA."); *Hoosier Contractors, LLC v. Gardner*, 212 N.E.3d 1234, 1240 (Ind. 2023), reh'g denied (Sept. 25, 2023) ("[T]he consumer must suffer an *actual injury* due to his reliance on a deceptive act."); *CFE Racing Prod., Inc. v. BMF Wheels, Inc.*, 2 F. Supp. 3d 1029, 1037 (E.D. Mich. 2014) (holding a plaintiff must suffer "actual loss" under the MCPA); *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1128 (W.D. Wash. 2012) (holding injury to "business or property" is a "crucial element of a CPA claim" and that "imminent threat to many users' information" is insufficient).

Thus, the Court dismisses these counts (Counts XI, XII, XV, XVI, XVIII) for failure to state a claim. Because the Court dismisses these counts for the reasons above, it finds it unnecessary to address the remaining arguments of Flagstar's Motion to Dismiss as to these counts. ECF No. 58, PageID.732-736.

IV.

Based on the foregoing, the Court holds that Plaintiffs have standing to pursue their claims, however, they fail to state a claim as to Counts I, II, III, IV, V, VI, VIII, X, XI, XII, XIII, XIV, XV, XVI, XVII, XVIII. Dismissal of Plaintiffs' claims as to these counts is warranted.

Accordingly, the Court **GRANTS** Defendant Flagstar's Motion to Dismiss as to Counts I, II, III, IV, V, VI, VII, VIII, X, XI, XII, XIII, XIV, XV, XVI, XVII, and

XVIII. The Court **DENIES** Defendant Flagstar's Motion to Dismiss as to its standing argument and Count IX.

IT IS SO ORDERED.

Dated: September 30, 2024

s/Brandy R. McMillion
BRANDY R. MCMILLION
United States District Judge